5. GRUPIŲ FAKTORIZACIJA

Grįžkime prie grupės A sluoksnių pogrupio B atžvilgiu.

5.24 apibrėžimas. *Grupės $(A,\cdot)$ pogrupis B vadinamas normaliuoju, jeigu visiems $a \in A$*

$$a \cdot B = B \cdot a.$$

5.25 pastaba. *Iš apibrėžimo matome, kad B – normalusis A pogrupis tada ir tik tada, kai $a \cdot B \cdot a^{-1} = B$ visiems $a \in A$. Ši sąlyga gali būti susilpninta:*

N) Grupės A pogrupis B yra normalusis tada ir tada, kai visiems $a \in A$

$$a \cdot B \cdot a^{-1} \subseteq B.$$

Nurodytas sąlygas įrodyti paliekame skaitytojui.

5.26 pavyzdžiai. 1. Bet koks komutatyviosios grupės pogrupis yra normalusis.

2. Grupės A pogrupis B, kurio indeksas $|A : B|$ grupėje A lygus 2, yra normalusis, nes grupės A tiek kairieji, tiek dešinieji sluoksniai B atžvilgiu yra tik du: B ir $A - B$.

Jeigu $A = S_n$ yra n-osios eilės simetrinė grupė, o $B = A_n$ – lyginių keitinių grupė (alternuojančioji grupė), tai, $|S_n| = n!$, $|A_n| = \frac{n!}{2}$. Pagal Lagranžo teoremą $|S_n : A_n| = \frac{n!}{n!/2} = 2$, todėl alternuojančioji grupė yra normalusis simetrinės grupės pogrupis.

Matyt, pati svarbiausia normaliųjų pogrupių savybė yra ta, kad grupės A sluoksnių normaliojo pogrupio B atžvilgiu aibėje (žymuo $A/_B$) galima apibrėžti grupės struktūrą. Parodysime, kaip tai padaryti.

5.27 teiginys. *Tegu $(A,\cdot)$ yra grupė, o $(B,\cdot)$ – jos normalusis pogrupis. Tada ekvivalentumo sąryšis $\sim$ iš 5.14 teiginio turi savybę:*

$$\textit{jeigu } a_1 \sim a_2 \textit{ ir } c_1 \sim c_2, \textit{ tai } a_1 \cdot c_1 \sim a_2 \cdot c_2,$$

t.y.,

$$\textit{jeigu } a_1 \cdot B = a_2 \cdot B \textit{ ir } c_1 \cdot B = c_2 \cdot B, \textit{ tai}$$

$$a_1 \cdot c_1 \cdot B = a_2 \cdot c_2 \cdot B;$$

čia a_1, a_2, c_1, c_2 *– bet kurie grupės* A *elementai.*

Teiginį įrodyti tiesiogiai paliekame skaitytojui kaip pratimą.

Šiuo teiginiu faktoraibėje $A/_B$ apibrėžiama operacija $\otimes$: $(a_1 \cdot B) \otimes (c_1 \cdot B) \overset{\text{def}}{=} (a_1 \cdot c_1) \cdot B$ yra korektiška, t.y. ji apibrėžiama sluoksniams ir nepriklauso nuo šiuos sluoksnius atstovaujančių elementų a_1 ir c_1 (juos galima pakeisti elementais a_2 ir c_2, kuriems teisinga $a_2 \sim a_1$, $c_2 \sim c_1$).

5.28 teiginys. *Jeigu* $(A, \cdot)$ *yra grupė, o* $(B, \cdot)$ *– jos normalusis pogrupis, tai* $(A/_B, \otimes)$ *yra grupė. Ši grupė vadinama grupės* A *faktorgrupe pogrupio* B *atžvilgiu.*

Įrodymas. 1) $G1$: $(a \cdot B) \otimes (c \cdot B) = (a \cdot c) \cdot B \in A/_B$ su visais $a, c \in A$.

2) $G2$:

$$\begin{aligned}\big((a \cdot B) \otimes (c \cdot B)\big) \otimes (d \cdot B) &= \big((a \cdot c) \cdot B\big) \otimes (d \cdot B) = \big((a \cdot c) \cdot d\big) \cdot B \\ &= \big(a \cdot (c \cdot d)\big) \cdot B = (a \cdot B) \otimes \big((c \cdot d) \cdot B\big) \\ &= (a \cdot B) \otimes \big((c \cdot B) \otimes (d \cdot B)\big).\end{aligned}$$

3) $G3$: jeigu 1 yra neutralusis grupės A elementas, tai $1 \cdot B = B$ – neutralusis $A/_B$ elementas: $(a \cdot B) \otimes (1 \cdot B) = (a \cdot 1) \cdot B = a \cdot B$, kai $a \in A$.

4) $G4$: jeigu a^{-1} yra atvirkštinis elemento a elementas grupėje A, tai

$$(a \cdot B) \otimes \big(a^{-1} \cdot B\big) = \big(a \cdot a^{-1}\big) \cdot B = 1 \cdot B = \big(a^{-1} \cdot a\big) \cdot B = \big(a^{-1} \cdot B\big) \otimes (a \cdot B).$$

$\triangle$

5.29 pastabos. 1. $|\,A/_B\,| = |A : B|$.

2. *Jeigu* A *yra baigtinė grupė, tai* $|\,A/_B\,| = \frac{|A|}{|B|}$.

5.30 pavyzdžiai. 1. Tegu $A = (S_n, \circ)$ yra simetrinė grupė, $B = (A_n, \circ)$ – alternuojanti grupė, $\circ$ – keitinių kompozicija.

Faktorgrupėje $\big(S_n/_{A_n}, \cdot\big)$, kurioje yra du elementai $\varepsilon = A_n$, $\alpha = S_n - A_n$, veiksmų lentelė yra

$\cdot$	ε	α
ε	ε	α
α	α	ε

2. Tegu $A = (\mathbb{Z}, +)$, $B = (n\mathbb{Z}, +)$, $n \in \mathbb{N}$.

Grupė A yra komutatyvioji grupė, todėl B – normalusis šios grupės pogrupis.

Remiantis 5.14 teiginiu, kai $a_1 \equiv c_1 \pmod{n}$, $a_2 \equiv c_2 \pmod{n}$, tai $a_1 + a_2 \equiv c_1 + c_2 \pmod{n}$.

Todėl $\left(\mathbb{Z}/_{n\mathbb{Z}}, \otimes\right) = \left(Z_n, +\right)$.

Grupių struktūrų teorijoje svarbus vaidmuo tenka funkcijoms, apibrėžtoms vienoje grupėje ir įgyjančioms reikšmes kitoje bei išlaikančioms šių struktūrų operacijas.

5.31 apibrėžimas. *Tegu $(A, *)$, $(B, \circ)$ yra grupės. Funkcija $f : A \to B$ vadinama grupių homomorfizmu, jeigu*

$$f(a_1 * a_2) = f(a_1) \circ f(a_2), \textit{su visais}\, a_1, a_2 \in A.$$

Bijektyvusis homomorfizmas vadinamas izomorfizmu.

5.32 pavyzdžiai. 1. $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(m) = \overline{m}$ yra homomorfizmas, nes $f(m_1 + m_2) = \overline{m_1 + m_2} = \overline{m_1} + \overline{m_2} = f(m_1) + f(m_2)$.

2. $A = GL_n(\mathbb{R})$ yra realiųjų n-osios eilės kvadratinių matricų multiplikacinė grupė, $B = \mathbb{R}^*$ – nenulinių realiųjų skaičių multiplikacinė grupė.

Funkcija $f(M) = \det\ M$ yra homomorfizmas, nes

$$f(M \cdot N) = \det(\ M \cdot N) = \det\ M \cdot \det\ N = f(M) \cdot f(N).$$

3. $A = S_n$ yra simetrinė grupė, $B = C_2$ – dviejų elementų $\{1, -1\}$ grupė su veiksmų lentele

$\cdot$	1	-1
1	1	-1
-1	-1	1

Funkcija

$$\operatorname{sign}(\pi) = \begin{cases} 1, & \text{kai } \pi \text{ – lyginis keitinys,} \\ -1, & \text{kai } \pi \text{ – nelyginis keitinys,} \end{cases}$$

yra homomorfizmas: $\operatorname{sign} : S_n \to C_2$.

Dabar pateiksime svarbiausias grupių homomorfizmų savybes.

5.33 teiginys. *Tegu* $(A, *)$, $(B, \cdot)$ *yra grupės,* e_A, e_B *– neutralieji grupių* A *ir* B *elementai, o* $f : A \to B$ *– grupių homomorfizmas. Tada:*
1) $\operatorname{Im} f = \{b \in B \mid \exists a \in A, f(a) = b\}$ *yra grupės* B *pogrupis.*
2) $f(e_A) = e_B$.
3) $f(a^{-1}) = ((f(a))^{-1}$, $a \in A$.

Įrodymas. 1) Sąlygas $G1 - G4$ aibei $\operatorname{Im} f$ patikrinti paliekame skaitytojui.
2) $f(a) = f(a * e) = f(a) \cdot f(e) = f(e * a) = f(e) \cdot f(a)$.
Taigi pagal neutraliojo elemento apibrėžimą $f(e_A) = e_B$.
3) $f(a) \cdot f(a^{-1}) = f(a^{-1}) \cdot f(a) = f(e)$, todėl

$$\begin{aligned}(f(a))^{-1} &= (f(a))^{-1} \cdot e_B = (f(a))^{-1} \cdot (f(a) \cdot f(a^{-1})) \\ &= ((f(a))^{-1} \cdot f(a)) \cdot f(a)^{-1} = e_B \cdot f(a^{-1}) = f(a^{-1}).\end{aligned}$$

△

5.34 apibrėžimas. *Tegu* $f : (A, *) \to (B, \circ)$ *yra grupių homomorfizmas. Aibė* $\operatorname{Ker} f = \{a \in A \mid f(a) = e_B$*; čia* e_B *– neutralus grupės* B *elementas*$\}$ *vadinama homomorfizmo* f *branduoliu.*

5.35 pavyzdžiai. 1. Homomorfizmo $f : \mathbb{Z} \to Z_n$, $f(m) = \overline{m}$, branduolys $\operatorname{Ker} f = \{m \in \mathbb{Z} \mid \overline{m} = \overline{0}\} = \{rn \mid r \in \mathbb{Z}\} =< n >$ – ciklinis $\mathbb{Z}$ pogrupis, generuojamas skaičiumi n.
2. Homomorfizmo $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ branduolys yra $\operatorname{Ker} \det = \{M \in GL_n(\mathbb{R}) \mid \det\ M = 1\} = SL_n(\mathbb{R})$ – specialioji tiesinė grupė.
3. Homomorfizmo $\operatorname{sign} : S_n \to C_2$ branduolys yra

$$\operatorname{Ker} \operatorname{sign} = \{\pi \mid \pi - \text{lyginis keitinys}\} = A_n - \text{alternuojančioji grupė.}$$

5.36 pastabos. 1. Grupių homomorfizmo $f : (A, *) \to (B, \cdot)$ branduolys $\operatorname{Ker} f$ yra normalusis pogrupis, nes jeigu $a \in A$, $c \in \operatorname{Ker} f$, tai

$$f(a * c * a^{-1}) = f(a) \cdot f(c) \cdot f(a^{-1}) = f(a) \cdot e_B \cdot f(a^{-1}) = f(a) \cdot f(a^{-1}) = e_B$$

ir todėl $a * c * a^{-1} \in \operatorname{Ker} f$. Taigi pagal sąlygą N) $\operatorname{Ker} f$ – normalusis pogrupis.

2. Svarbu yra ir tai, kad jeigu N yra grupės $(A, *)$ normalusis pogrupis, tai galima apibrėžti homomorfizmą

$$f : A \to A/_{N},$$
$$f(a) = a * N,$$

kurio branduolys $\operatorname{Ker} f = N$.

Kitais žodžiais sakant, bet kuris grupių homomorfizmo branduolys yra normalusis pogrupis ir kiekvieną normalųjį grupės pogrupį galima realizuoti kaip visiškai apibrėžto homomorfizmo branduolį. Šiuos samprotavimus apibendrina 3.13 teiginio analogas grupėms.

5.37 teorema (homomorfizmų teorema grupėms). *Tegu $f : (A, *) \to (B, \circ)$ yra grupių homomorfizmas. Tada egzistuoja vienintelis homomorfizmas $\overline{f} : A/_{\operatorname{Ker} f} \to B$, kurio dėka diagrama*

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "p"'] & & B \\ & A/_{\operatorname{Ker} f} \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

yra komutatyvi, t.y. $f = \overline{f} \cdot p$, $\overline{f}$ yra grupių $\left(A/_{\operatorname{Ker} f}, \otimes\right)$ ir $f(A)$ izomorfizmas, o p – siurjektyvusis homomorfizmas.

5.38 apibrėžimas. *Grupės A ir B vadinamos izomorfinėmis, jeigu egzistuoja izomorfizmas $f : A \to B$. Žymėsime $A \approx B$.*

5.39 pastabos. 1. Grupių izomorfizmas yra ekvivalentumo sąryšis.

2. Jeigu funkcija $f : A \to B$ yra grupių A ir B izomorfizmas, tai ir funkcija $f^{-1} : B \to A$ yra grupių B ir A izomorfizmas.

5.40 pavyzdžiai. 1. $\mathbb{Z}/_{\langle n \rangle} \approx \mathbb{Z}_n$. Įdomu yra ir tai, kad ciklinis sveikųjų skaičių grupės $(\mathbb{Z}, +)$ pogrupis $\langle n \rangle \approx \mathbb{Z}$: iš tikrųjų funkcija $f_n : \mathbb{Z} \to \langle n \rangle$, $f_n(m) = n \cdot m$, yra grupių izomorfizmas. Atkreipkime dėmesį ir į tai, kad $(\mathbb{Z}, +)$ ir $\langle n \rangle$ yra abi begalinės ciklinės grupės, kurių generuojantys elementai 1 arba -1 yra grupėje $\mathbb{Z}$ ir n arba $-n$ – grupėje $\langle n \rangle$.

2. $S_n/_{A_n} \approx C_2$.

3. $GL_n(\mathbb{R})/_{SL_n(\mathbb{R})} \approx \mathbb{R}^*$.

4. Pradėsime apibrėžimu. Tegu $(A, *)$ ir $(B, \circ)$ yra grupės. Algebrinė struktūra

$$(A \times B, \cdot),$$

kuriai apibrėžta

$$\big(a_1, b_1\big) \cdot \big(a_2, b_2\big) = \big(a_1 * a_2, b_1 \circ b_2\big),$$

vadinama *grupių A ir B tiesiogine sandauga.*

Tai, kad tiesioginė grupių sandauga yra grupė, paliekame patikrinti skaitytojui. Pateiksime įdomų pavyzdį.

Grupėje $\mathbb{Z}_2 \times \mathbb{Z}_3$ yra šeši elementai:

$$(0,0), (0,1), (0,2), (1,0), (1,1) \text{ ir } (1,2).$$

Veiksmų lentelė šioje grupėje yra tokia:

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Nesudėtinga įsitikinti tuo, kad funkcija $f : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$, apibrėžta lygybėmis $f(\overline{0}) = (0,0)$, $f(\overline{1}) = (1,1)$, $f(\overline{2}) = (0,2)$, $f(\overline{3}) = (1,0)$, $f(\overline{4}) = (0,1)$, $f(\overline{5}) = (1,2)$, yra grupių izomorfizmas: $\mathbb{Z}_6 \approx \mathbb{Z}_2 \times \mathbb{Z}_3$.

Bet ar izomorfinės grupės $\mathbb{Z}_8$ ir $\mathbb{Z}_2 \times \mathbb{Z}_4$? Jei ne, tai kodėl, jei taip, tai kodėl?

Nagrinėkime ciklines grupes.

Pasirodo, kad visos ciklinės grupės yra izomorfiškos arba sveikųjų skaičių grupei $\mathbb{Z}$, arba vienai iš grupių $\mathbb{Z}_n$, $n \in \mathbb{N}$, priklausomai nuo to, ar kalbama apie begalinę, ar apie baigtinę ciklinę grupę.

5.41 teiginys. *1. Baigtinė ciklinė grupė, kurioje yra n elementų, yra izomorfinė grupei $\mathbb{Z}_n$:*

$$\langle a\rangle_n = \big(\{a, a^2, \ldots, a^n = e\}, \cdot\big) \approx (zzm_n, +)$$

2. Begalinė ciklinė grupė yra izomorfinė grupei $\mathbb{Z}$.

Įrodymas. 1. Funkcija $\varphi_n : \mathbb{Z}_n \to \langle a\rangle_n$, apibrėžta lygybe $\varphi_n(\overline{k}) = a^k$, yra izomorfizmas:

a) φ_n – homomorfizmas, nes $\varphi_n(\overline{k} + \overline{l}) = a^k \cdot a^l = \varphi_n(\overline{k}) \cdot \varphi_n(\overline{l})$;

b) φ_n – bijekcija, nes, jeigu $\varphi_n(\overline{k}) = \varphi_n(\overline{l})$, tai $a^k = a^l$ ir todėl $k = l$, kai $1 \leqslant k, l \leqslant n$.

2. Funkcija $\varphi_0 : \mathbb{Z} \to \langle a\rangle)$, apibrėžta lygybėmis $\varphi_0(k) = a^k$, yra izomorfizmas:

a) φ_0 – homomorfizmas, nes $\varphi_0(k+l) = a^{k+l} = a^k \cdot a^l = \varphi_0(k) \cdot \varphi_0(l)$;

b) φ_0 – bijekcija, nes $\varphi_0(k) = \varphi_0(l)$ tada ir tik tada, kai $a^k = a^l$, $a^{k-l} = e_{\langle a\rangle}$, t.y. $k - l = 0$, $k = l$.

$\triangle$

5.42 pavyzdys. Ciklinė grupė visada komutatyvi, nes ir $\mathbb{Z}$, ir $\mathbb{Z}_n$ yra komutatyvios grupės. Štai kodėl simetrinė grupė S_n, $n \geqslant 3$, nėra ciklinė: ji nėra komutatyvi: $(12)(123) = (13) \neq (23) = (123)(12)$.